PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04Q 7/00

A2

(11) Internationale Veröffentlichungsnummer: WO 99/03285

(43) Internationales Veröffentlichungsdatum: 21. Januar 1999 (21.01.99)

(21) Internationales Aktenzeichen: PCT/DE98/01922

(22) Internationales Anmeldedatum: 10. Juli 1998 (10.07.98)

(30) Prioritätsdaten:

197 29 611.4	10. Juli 1997 (10.07.97)	DE
197 30 301.3	15. Juli 1997 (15.07.97)	DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DE-TEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH [DE/DE]; Landgrabenweg 151, D–53227 Bonn (DE).

(71) Anmelder *(nur für US)*: PERNICE, Edith (Erbin des verstorbenen Erfinders) [DE/DE]; Schillerstrasse 11, D–64846 Groß–Zimmern (DE).

(72) Erfinder: PERNICE, Frieder (verstorben).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: MARINGER, Günter [DE/DE]; Troschelstrasse 8, D–53115 Bonn (DE). MOHRS, Walter [DE/DE]; Rosenhain 3, D–53123 Bonn (DE).

(74) Anwalt: RIEBLING, Peter; Postfach 3160, D–88113 Lindau (DE).

(81) Bestimmungsstaaten: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CZ, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: METHOD AND DEVICE FOR THE MUTUAL AUTHENTICATION OF COMPONENTS IN A NETWORK USING THE CHALLENGE–RESPONSE METHOD

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR GEGENSEITIGEN AUTHENTISIERUNG VON KOMPONENTEN IN EINEM NETZ MIT DEM CHALLENGE–RESPONSE–VERFAHREN

(57) Abstract

The invention relates to a method for the mutual authentication of components in a network by means of the challenge–response method, according to which the network (N) requests a set of three data values (challenge 1/ response 1/ response 2) from an authentication centre (AUC) and transmits at least one set of data values (challenge 1) to the mobile station (M) which on the basis of an internally stored key (Ki) calculates a response 1 from this set of data values and transmit it to the network (N). To authenticate the network (N) in relation to the mobile station (M) the invention provides for the response 1 sent back to the network (N) to be interpreted simultaneously by said network (N) as challenge 2 and for said network (N) immediately to transmit a response 2 to the mobile station (M). This improves and accelerates data traffic between the mobile station and the network because there is no transmission of challenge 2 between the mobile station and the network. Data traffic between the network and the AUC is also improved because the data pairs challenge 2 and response 2 no longer have to be calculated separately in the AUC and transmitted to the network.

(57) Zusammenfassung

Es wird ein Verfahren zur gegenseitigen Authentisierung von Komponenten in einem Netz nach dem Challenge–Response–Verfahren beschrieben, bei dem das Netz (N) von einem Authentisierungszentrum (AUC) einen Dreier–Datensatz (Challenge 1/Response 1/Response 2) anfordert und mindestens einen Datensatz (Challenge 1) an die Mobilstation weiterleitet, welche aufgrund eines intern gespeicherten Schlüssels (Ki) hieraus eine Response 1 berechnet und an das Netz (N) absendet. Zur Authentisierung des Netzes (N) gegenüber der Mobilstation (M) ist vorgesehen, daß die an das Netz (N) zurückgesandte Response 1 gleichzeitig vom Netz (N) als Challenge 2 interpretiert wird, und daß das Netz (N) hierauf sofort eine Response 2 an die Mobilstation (M) sendet. Hierdurch wird der Datenverkehr zwischen der Mobilstation und dem Netz verbessert und beschleunigt, denn es wird auf die Übertragung der Challenge 2 zwischen Mobilstation und Netz verzichtet. Ebenso wird der Datenverkehr zwischen dem Netz und dem AUC verbessert, denn die Datenpaare Challenge 2 und Response 2 müssen nicht mehr im AUC gesondert berechnet und an das Netz weitergeleitet werden.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Verfahren und Vorrichtung zur gegenseitigen Authentisierung von Komponenten in einem Netz mit dem Challenge-Response-Verfahren.

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur gegenseitigen Authentisierung von Komponenten in einem Netz mit dem Challenge-Response-Verfahren nach dem Oberbegriff des Anspruches 1. Insbesondere betrifft die Erfindung die gegenseitige Authentisierung eines Endgeräts, bevorzugt einer Mobilstation gegenüber dem Netz und umgekehrt. Im folgenden wird der Begriff „Mobilstation" verwendet; dies ist nicht einschränkend zu verstehen. Hierunter sollen alle möglichen Endgeräte fallen, auch stationäre, wie z.B. einzelne Nutzer eines Computers in einem drahtgebundenen System.

Authentisieren dient zur Überprüfung der Echtheit der zu authentisierenden Komponente.
Stand der Technik ist das sogenannte Challenge-Response-Verfahren: Bei diesem wird von der authentisierenden Komponente (N = Netz) eine Zufallszahl (Challenge) an die zu authentisierende Komponente (M = Mobilstation) gesandt, die mit Hilfe eines Algorithmus (A) und eines geheimen, beiden Komponenten bekannten Schlüssels K in eine Antwort (Response) umgerechnet wird. Im Netz N wird mit gleichem Schlüssel K und dem gleichen Algorithmus A die erwartete Response errechnet; eine Übereinstimmung der von M zurückgesendeten mit der bei N errechneten Response beweist die Echtheit von M.
Eine gegenseitige Authentisierung wird nach Stand der Technik dadurch erreicht, daß der obige Ablauf mit umgekehrter Rollenverteilung stattfindet.

Bei dem bekannten Challenge-Response-Verfahren gibt demnach das Festnetz eine Challenge an die Mobilstation M und die

Mobilstation M antwortet mit einer Response, die aus einem Rechenverfahren errechnet wurde, das in der Mobilstation implementiert ist und zu der ein geheimer Schlüssel K gehört. Dieser Schlüssel K ist einmalig. D. h. nur diese Mobilstation kann so antworten, wie es von ihr erwartet wird, sofern sie "echt" = authentisiert ist. Eine andere Mobilstation (M) kann diesen Schlüssel nicht simulieren.

Nachteil des bisherigen Verfahrens ist, daß das gesamte Authentisierungsverfahren nur und ausschließlich in der AUC (Authentisierungszentrale), das heißt praktisch in der Rechenzentrale, verifiziert werden kann.

Aus Sicherheitsgründen hat es sich nämlich in Systemarchitekturen als vorteilhaft erwiesen, A und K an zentraler Stelle (im Authentication Center = AUC) zu verwalten, wobei der authentisierenden (die Echtheitsprüfung durchführenden) Stelle N zum Zwecke der Authentisierung nur Challenge/Response-Paare im voraus (ggf. mehrere auf Vorrat) übertragen werden.

Die vom AUC in das Netz (auf Anforderung des Netzes in Form eines sogenannten „Duplet Request") übergebenen Challenge/Response-Paare werden also in großem Umfang bereits schon „auf Vorrat" errechnet und wenn während des Authentisierungsvorgangs die Antwort (Response) von der Mobilstation M kommt, werden beide Anworten verglichen. Bei Übereinstimmung ist damit das Authentisierungsverfahren der Mobilstation M gegenüber dem Netz N erfolgreich beendet.

Bei den bekannten Verfahren des Standes der Technik ist demnach vorgesehen, daß sich die Mobilstationen gegenüber dem Netz authentisieren. Es besteht damit die Gefahr, daß von Unbefugten

das Netz simuliert wird und daß damit die betreffende Mobilstation M an das simulierte Netz „angelockt" wird und hierbei der Mobilstation M vorgespiegelt wird, es handele sich hierbei um das „richtige" Netz N. Für diesen unerlaubten Fall würde sich die M gegenüber dem simulierten Netz N authentisieren und damit kann der unbefugte Betreiber des simulierten Netzes nichtöffentliche Daten aus dieser Mobilstation M abrufen.

Als Beispiel sei das GSM-Netz genannt, das bisher nur eine einseitige Authentisierung. vornimmt (M authentisiert sich gegenüber N). Beim ferner bekannten TETRA-Standard, ist eine zweiseitige Authentisierung erlaubt.

Zur besseren Verdeutlichung der später verwendeten Begriffe „Challenge 1, Response 1 und Challenge 2, Resonse 2", wird nachfolgend das Verfahren erläutert:

Die Challenge 1 dient der Authentikation der Mobilstation M gegenüber dem Netz N. Sobald diese Authentikation erfolgreich abgeschlossen wurde, fordert die Mobilstation M eine umgekehrte Authentifizierung, in der Weise, daß jetzt geprüft wird, ob das derzeitige Netz N auch wirklich das befugte Netz ist und nicht ein unerlaubterweise simuliertes Netz. Es soll sich also das Netz N gegenüber der Mobilstation M authentisieren. Die Mobilstation M schickt hierbei eine Challenge 2 zum Netz, dieses leitet die Challenge 2 zum AUC weiter, wo daraus die Response 2 errechnet wird, die wiederum an das Netz N geschickt wird, welches Response 2 an die Mobilstation weiterleitet. Hat die Mobilstation die Übereinstimmung von der selbst berechneten Response 2 und der erhaltenen Response 2 festgestellt, ist damit die Authentifizierung erfolgreich beendet. Dieses Authentifizierungspaar wird als Challenge 2/Response 2 bezeichnet.

Bei gegenseitiger Authentisierung wirkt sich in solchen Systemarchitekturen nachteilig aus, daß die von M gesandte Challenge nicht in N, sondern nur im AUC in die Response umgerechnet werden kann, was unter Umständen zu erheblichen Zeitverzögerungen wegen des Datentransfers N-AUC-N und der online Rechenoperation im AUC führt.

Der Erfindung liegt die Aufgabe zugrunde, das bekannte Verfahren zur Authentifikation von Komponenten in einem Netz, insbesondere in einem GSM-Netz, so zu verbessern, daß dieses Verfahren wesentlich beschleunigt wird.

Zur Lösung der gestellten Aufgabe ist das Verfahren dadurch gekennzeichnet, daß die von der Mobilstation M zurückgesandte Response 1 gleichzeitig von dem Netz N als Challenge 2 verwendet wird, was den Vorteil hat, daß vom AUC gleichzeitig mit den o.g. Challenge/Response-Paaren auch die Response 2 (als Antwort auf Challenge 2) errechnet und übermittelt wird. Dadurch entfällt die Zeitverzögerung, die auftreten würde, wenn N sich Response 2 erst nach Eintreffen von Challenge 2 beim AUC besorgen müßte.

Damit ist vorgesehen, daß die Mobilstation zur Echtheitserkennung des Netzes N nicht mehr eine Challenge 2 intern erzeugt und an das Netz schickt, sondern daß durch Gleichsetzen der Response 1 mit der Challenge 2 schon gegenseitige Übereinstimmung in M und N über die erwartete Challenge 2 existiert. Das Netz kann somit schon eine Response 2 erzeugen und an die Mobilstation schicken, welche diese Response 2 mit dem bei sich errechneten Wert vergleicht und bei Übereinstimmung das Netz als „echt" anerkennt.

Wichtig hierbei ist also , daß man die von der Mobilstation an das Netz abgeschickte Response 1 gleichzeitig als Challenge 2 dieser Mobilstation benutzt, welche diese aber nicht mehr in das Netz schickt, um auf die Response 2 des Netzes wartet. Die Challenge 2 der Mobilstation kennt das Netz nämlich schon vorher, weil die Response 2 intern bereits schon berechnet wurde. Damit kann das Netz bereits auch schon die Response 2 errechnen.

Erfindungsgemäß laufen die wechselseitige Authentifikation von Mobilstation zum Netz und danachfolgend die Authentifikation von Netz zur Mobilstation nun nicht mehr mit relativ hohem Zeitbedarf zeitlich aufeinanderfolgend ab, sondern die beiden Echtheitsprüfungen werden nun zeitlich miteinander verzahnt.

Es wird damit eine vollständige Datenübertragung einer Prüfzahl (Challenge 2) vermieden, denn erfindungsgemäß kann die Challenge 2 eingespart werden und muß nicht mehr übertragen werden. Die separate Übertragung der Response 2 vom Netz wird dadurch eingespart, als das Netz gleich bei Absendung von Challenge 1 auch bereits schon die Response 2 zur Mobilstation schickt. Begründet wird dies damit, daß das Netz schon vorher weiß, was die Challenge 2 der Mobilstation sein wird, also kann das Netz auch sofort die Response 2 zur Mobilstation schicken. In einer einzigen Datenübertragung überträgt das Netz also die Datenpaarung Challenge 1 / Response 2 zur Mobilstation. Damit wird erreicht, daß die Mobilstation die Echtheit von N bereits erkannt hat, bevor sich M gegenüber N authentisiert hat.

Hierbei gibt es zwei verschiedene Ausführungen :

In einer ersten Ausführungsform übermittelt das Netz an die Mobilstation die Challenge 1. Die Mobilstation M antwortet mit Response 1. Nachdem dem Netz vom AUC vorher aber bereits eine Vielzahl von Dreier-Datenpaketen (Triplet= Challenge 1/ Response 1 / Response 2) übermittelt wurden, kennt das Netz N auch die Response 1 der Mobilstation M im voraus. Mit Kenntnis von Response 1 ist ihm aber auch die Challenge 2 bekannt. Die Mobilstation sendet nun nicht mehr die Challenge 2 zum Netz, sondern das Netz antwortet auf die Response 1 von M mit der Response 2. Diese Kenntnis ist jedoch nur dem „echten" Netz zu eigen; ein simuliertes, unerlaubtes Netz hat diese Kenntnis nicht; damit hat sich das Netz N gegenüber der Mobilstation durch die Übertragung eines einzigen Datenpaktes (Challenge 1 / Response 2) authentisiert und erspart sich die Übertragung des zweiten Datenpaketes (Challenge 2).

Hierbei ist vorteilhaft, daß die Response 2 eine Funktion von Response 1 ist. Das heißt, bei Kenntnis des Funktionszusammenhangs kann aus der Response 1 = Challenge 2 die Response 2 berechnet werden. Nach dem Stand der Technik war die Response 2 eine Funktion von Challenge 2. Erfindungsgemäß muß Challenge 2 nicht mehr übertragen werden, da Challenge 2 = Response 1 eine Funktion von Challenge 1 ist.

Letztendlich gilt durch die Gleichsetzung von Response 1 und Challenge 2, daß Response 2 auch eine Funktion von Challenge 1 ist.

In der ersten Ausgestaltung werden demgemäß Challenge 1 und Response 2 zeitlich hintereinander folgend an die Mobilstation M geschickt.

In einer zweiten Ausgestaltung ist es vorgesehen, daß Challenge 1 und Response 2 als ein Datenpaket zusammen an die Mobilstation M geschickt werden.
Hierauf antwortet die Mobilstation mit Response 1 und jetzt vergleicht das Netz Response 1 mit dem erwarteten Wert von Response 1 und die Mobilstation vergleicht Response 2 mit dem intern errechneten Wert von Response 2.

In bekannten Systemen (z..B. im GSM-Netz) ist die Länge der Response (32 bit) kürzer als die Zufallszahl Challenge (128 bit). Um die Response gleichzeitig als Challenge zur Authentisierung von N gegenüber M mit dem gleichen Algorithmus A benutzen zu können, ist es notwendig, die Länge von Response 1 auf die von Algorithmus A erwartete Länge von 128 bit zu erhöhen.
Dies könnte durch vierfache Verkettung von Response 1 (4 x 32 bit = 128 bit) oder durch vorher definiertes (teilnehmerindividuelles oder teilnehmerunabhängiges) Auffüllen auf 128 bit erreicht werden.

Vorschläge für das teilnehmerindividuelle Auffüllen sind:

1 . Hernahme des kompletten Rechenergebnisses von Response 1 , bevor es zur Übertragung zur Gegenstelle auf 32 bit verkürzt wurde

2.. Auffüllen mit definierten Bits aus dem in M und AUC bekannten K_i.

Der Vorteil beider Ausführungsformen gegenüber dem Stand der Technik liegt also darin, daß der Datenverkehr zwischen dem Netz und der Mobilstation einerseits und auch der Datenverkehr zwischen dem Netz und der AUC vereinfacht und damit beschleunigt wird. Nach dem Stand der Technik müssen vier Telegramme zwischen Netz und Mobilstation M hin und

hergeschickt werden, nämlich Challenge 1, Response 1, Challenge 2 und Response 2.
Außerdem muß das Netz die Challenge 2 erst an das AUC übermitteln und dieses muß die Response 2 errechnen und an das Netz übergeben, was mit weiterem Zeitverlust verbunden ist.

Erfindungsgemäß wird eine zeitaufwendige Online-Abfrage vom Netz an die AUC vermieden. Dies erfolgt dadurch, daß bereits schon vor dem eigentliche Datenverkehr zur Authentifizierung zwischen Netz und Mobilstation die von der AUC hierfür benötigten Datenpakete abgerufen und beim Netz zur späteren Verwendung zwischengespeichert werden.

Derartige Datenpakte (Triplets) können schon in großem zeitlichen Vorlauf (z. B. Stunden oder Tage vorher) vom Netz vom AUC abgerufen werden. Allen beiden Ausführungen ist hierbei gemeinsam, daß man die Response 1 als Challenge 2 benutzt und damit auf die eigentliche Übermittlung von Challenge 2 verzichten kann.

Mehrere bevorzugte Ausführungsbeispiele werden nun anhand der Zeichnungen näher beschrieben. Hierbei gehen aus der Zeichnung und ihrer Beschreibung weitere Merkmale der Erfindung hervor.
Es zeigen :
Fig. 1 : Schematisiert ein Authentifizierungsverfahren nach dem Stand der Technik
Fig. 2 : Eine erste Ausführungsform der Authentifizierung nach der Erfindung
Fig. 3 : Eine zweite Ausführungsform der Authentifizierung nach der Erfindung

In der Ausführung nach Fig. 1 fordert zunächst das Netz N Datensätze als Zweier-Pakete (Duplet-Request) von der AUC an.

Diese Zweier-Pakete enthalten die Datensätze für Challenge 1/Response 1. Sobald sich nun eine Mobilstation M gegenüber dem Netz N authentifizieren soll, sendet N zunächst den Datensatz Challenge 1 an M, welche mit Response 1 antwortet. Falls N eine Übereinstimmung beider Datensätze feststellt, wurde damit die „Echtheit" von M gegenüber N erwiesen. Umgekehrt fordert nun M die Echtheitsprüfung von N dadurch, daß M an N eine Challenge 2 sendet, welche N an AUC weiterleitet, wo daraus die geforderte Response 2 berechnet wird, die AUC an N weitergibt, die dieses wiederum an M absendet. M vergleicht nun die intern berechnete und die von N erhaltene Response 2 und erkennt bei Übereinstimmung beider die Echtheit von N an.

Wie bereits schon eingangs darauf hingewiesen, wird durch diesen vielfältigen Datenaustausch der Verkehr zwischen M und N einerseits und N und AUC andererseits stark belastet und ist daher mit Zeitverzögerungen behaftet.
Hier greift das neue Verfahren in seiner ersten Ausführung gemäß Fig. 2 ein, wo vorgesehen ist, daß N von AUC sogenannte Dreier-Datensätze (Triplets) in Form von Challenge 1/Response 1/Response 2 fordert. Hierbei ist der Datensatz Response 2 eine definierte Funktion des Datensatzes Response 1 und durch einen Algorithmus berechenbar. Derartige Datensätze werden zeitlich längst vor der Abwicklung des Datenverkehrs von N mit M von AUC abgefordert und in Form von Vielfach-Datensätzen in N gespeichert. Hierdurch entfällt die Notwendigkeit des Online-Datenverkehrs zwischen N und AUC, wie es beim Stand der Technik nach Figur 1 notwendig gewesen war.
Zur Authentifizierung von M gegenüber N sendet N an M zunächst die Challenge 1, worauf M mit der Response 1 antwortet. Nachdem N bereits schon den Datensatz Challenge 2 kennt, der beim Stand der Technik von M an N gesendet wird, reicht es aus, wenn N zur Authentifizierung gegenüber M nur noch den Datensatz Response 2

an M sendet. M hat intern den Datensatz Response 2 errechnet und vergleicht diesen mit der von N gesendeten Response 2. Bei Übereinstimmung ist damit die „Echtheit" von N gegenüber M erwiesen.

In der zweiten Ausführungsform des Verfahrens nach Figur 3 ist in Abweichung des Verfahrens nach Figur 2 vorgesehen, daß N sofort und einmalig den Datensatz Challenge 1/Response 2 an M schickt. Sobald M den Datensatz Response 1 zurückschickt ist damit sowohl die Authentifizierung von M gegenüber N als auch umgekehrt von N gegenüber M gelungen.

Patentansprüche

1.Verfahren zur gegenseitigen Authentisierung von Komponenten in einem Netz nach dem Challenge-Response-Verfahren, bei dem zur Authentifizierung eines Endgeräts, insbesondere einer Mobilstation, gegenüber dem Netz das Netz (N) von einem Authentisierungszentrum (AUC) aufgrund einer Anforderung mindestens ein Datenpaar (Challenge 1, Response 1) anfordert und den Datensatz (Challenge 1) an das Endgerät (M) weiterleitet, welche aufgrund eines intern gespeicherten Schlüssels (Ki) hieraus eine Response 1 berechnet und an das Netz (N) absendet, wobei ferner eine Authentisierung des Netzes (N) gegenüber dem Endgerät (M) stattfindet, **dadurch gekennzeichnet, daß** anstatt der Anforderung von einem Datenpaar (Challenge 1 / Response 1) vom Netz N an das AUC nunmehr ein Dreier-Datensatz (Challenge 1 / Response 1 / Response 2) vom Netz vom AUC angefordert wird und daß die von dem Endgerät (M) an das Netz (N) gesandte Challenge 2 identisch ist mit der Response 1, und daß das Netz (N) hierauf ein Response 2 an das Endgerät (M) sendet.

2.Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß auf die Übertragung von Challenge 2 verzichtet wird und daß das Netz die von dem Endgerät (M) zurückgesandte Response 1 als Challenge 2 interpretiert.

3.Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, daß** die Übertragung des Datenpaares (Challenge 1/ Response 2) von dem Netz (N) zu dem Endgerät (M) gleichzeitig in Form eines einzigen Datensatzes erfolgt, (Fig. 3).

4.Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, daß die Übertragung des Datenpaares (Challenge 1/Response 2) von dem Netz (N) zu dem Endgerät(M) gleichzeitig in Form eines einzigen Datensatzes erfolgt, (Fig. 3).

5.Verfahren nach einem der Ansprüche 2, 3 oder 4, **dadurch gekennzeichnet, daß** das Netz Datensätze vom Authentifizierungszentrum (AUC) in Form von Dreier-Datensätzen (Challenge 1/Response 1/Response 2) anfordert.

6.Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß zur Herabsetzung der Anforderungshäufigkeit mehrere Dreier-Datensätze vom AUC als Vorrat geliefert werden.

7.Verfahren nach Anspruch 4 oder 5, **dadurch gekennzeichnet, daß** zur Verwendung der Response 1 des Endgeräts (M) als Challenge zwecks Authentifikation des Netzes gegenüber dem Endgerät (M) die kürzere Länge der Response 1 auf die größere Länge der Challenge aufgefüllt wird.

8.Verfahren nach Anspruch 7, **dadurch gekennzeichnet, daß** das Auffüllen teilnehmer-individuell erfolgt und daß die

vollständige Länge der Response 1 vor der Übertragung auf die Gegenstelle verkürzt wird.

9. Verfahren nach Anspruch 8, **dadurch gekennzeichnet**, daß die Response 1 mit definierten Bits aus dem geheimen Schlüssel Ki auf die Länge der Challenge 2 aufgefüllt wird.

10. Verfahren nach Anspruch 8, **dadurch gekennzeichnet**, daß die Challenge der originalen Response 1 vor ihrer Kürzung entspricht.

11. Verwendung des Verfahrens nach einem der Ansprüche 1 - 10, **dadurch gekennzeichnet**, daß das Netz ein GSM-Netz ist.

12. Verwendung des Verfahrens nach einem der Ansprüche 1 - 10, **dadurch gekennzeichnet**, daß das Netz ein drahtgebundenes Netz ist.

13. Verwendung nach Anspruch 12, **dadurch gekennzeichnet**, daß die einzelnen, sich gegenseitig authentisierenden Komponenten in einem drahtgebundenen Netz verschiedene Kontrolleinheiten von Computern sind, welche sich gegenüber einem Zentralcomputer authentifizieren und umgekehrt.

14. Vorrichtung zur gegenseitigen Authentisierung von Komponenten in einem Netzwerk nach einem der Ansprüche 1 -. 13, **dadurch gekennzeichnet**, daß das AUC die vom Netz geforderten Dreier-Datensätze berechnet und auf Anforderung vom Netz diese Off-Line und zeitlich unabhängig, jedoch auf jeden Fall vor dem Datenaustausch zwischen Netz und Endgerät an das Netz übermittelt.

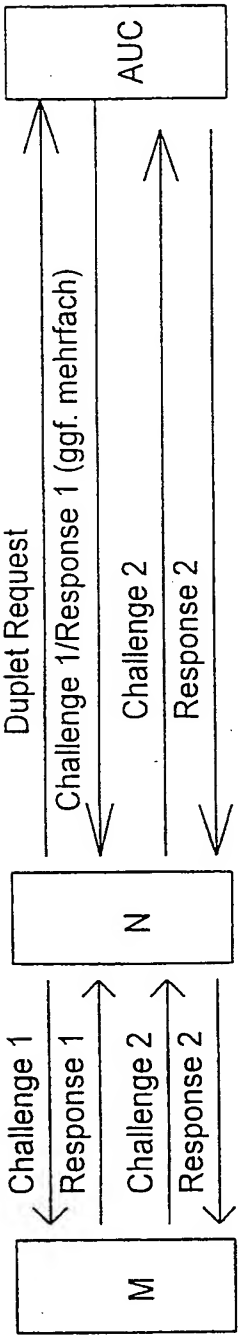


Fig. 1

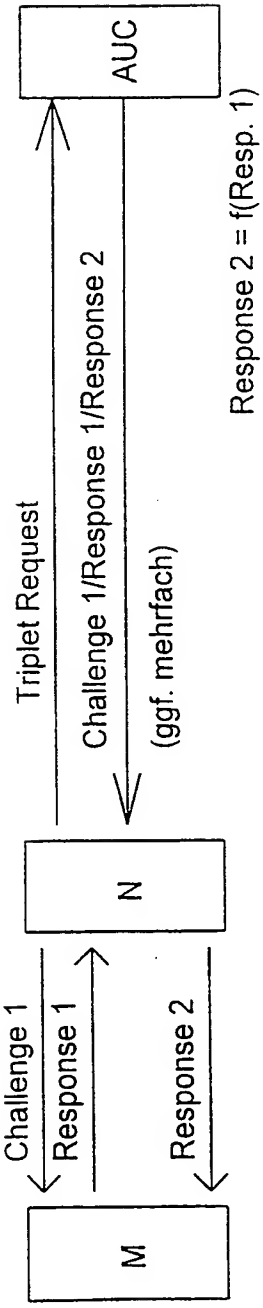


Fig. 2

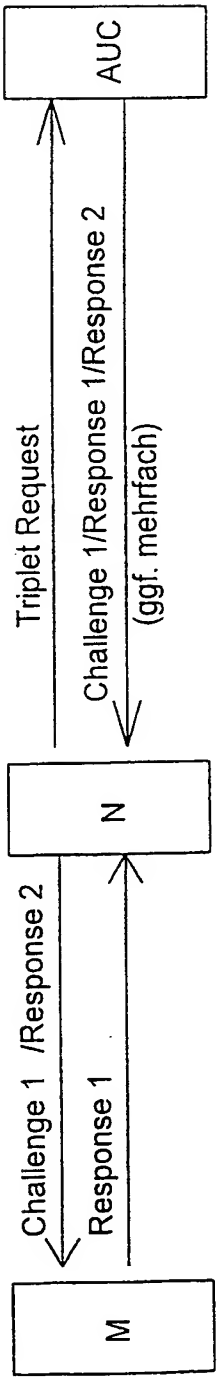


Fig. 3

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

PCT

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04L 9/32, H04Q 7/38

A3

(11) Internationale Veröffentlichungsnummer: WO 99/03285

(43) Internationales Veröffentlichungsdatum: 21. Januar 1999 (21.01.99)

(21) Internationales Aktenzeichen: PCT/DE98/01922

(22) Internationales Anmeldedatum: 10. Juli 1998 (10.07.98)

(30) Prioritätsdaten:

197 29 611.4	10. Juli 1997 (10.07.97)	DE
197 30 301.3	15. Juli 1997 (15.07.97)	DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DE-TEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH [DE/DE]; Landgrabenweg 151, D–53227 Bonn (DE).

(71) Anmelder *(nur für US)*: PERNICE, Edith (Erbin des verstorbenen Erfinders) [DE/DE]; Schillerstrasse 11, D–64846 Groß–Zimmern (DE).

(72) Erfinder: PERNICE, Frieder (verstorben).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: MARINGER, Günter [DE/DE]; Troschelstrasse 8, D–53115 Bonn (DE). MOHRS, Walter [DE/DE]; Rosenhain 3, D–53123 Bonn (DE).

(74) Anwalt: RIEBLING, Peter; Postfach 3160, D–88113 Lindau (DE).

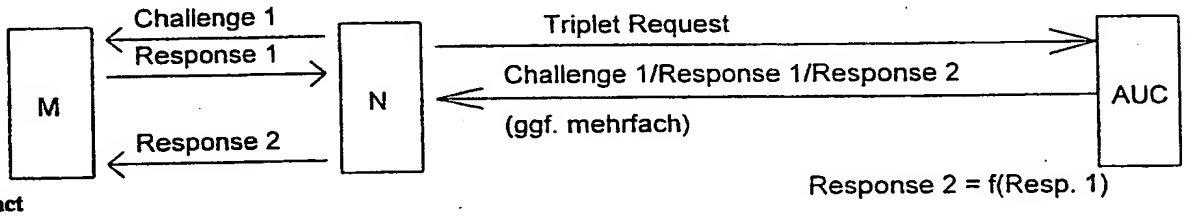
(81) Bestimmungsstaaten: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CZ, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Mit internationalem Recherchenbericht.

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 1. April 1999 (01.04.99)

(54) Title: METHOD AND DEVICE FOR THE MUTUAL AUTHENTICATION OF COMPONENTS IN A NETWORK USING THE CHALLENGE–RESPONSE METHOD

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR GEGENSEITIGEN AUTHENTISIERUNG VON KOMPONENTEN IN EINEM NETZ MIT DEM CHALLENGE–RESPONSE–VERFAHREN



(57) Abstract

The invention relates to a method for the mutual authentication of components in a network by means of the challenge–response method, according to which the network (N) requests a set of three data values (challenge 1/ response 1/ response 2) from an authentication centre (AUC) and transmits at least one set of data values (challenge 1) to the mobile station (M) which on the basis of an internally stored key (Ki) calculates a response 1 from this set of data values and transmit it to the network (N). To authenticate the network (N) in relation to the mobile station (M) the invention provides for the response 1 sent back to the network (N) to be interpreted simultaneously by said network (N) as challenge 2 and for said network (N) immediately to transmit a response 2 to the mobile station (M). This improves and accelerates data traffic between the mobile station and the network because there is no transmission of challenge 2 between the mobile station and the network. Data traffic between the network and the AUC is also improved because the data pairs challenge 2 and response 2 no longer have to be calculated separately in the AUC and transmitted to the network.

(57) Zusammenfassung

Es wird ein Verfahren zur gegenseitigen Authentisierung von Komponenten in einem Netz nach dem Challenge–Response–Verfahren beschrieben, bei dem das Netz (N) von einem Authentisierungszentrum (AUC) einen Dreier–Datensatz (Challenge 1/Response 1/Response 2) anfordert und mindestens einen Datensatz (Challenge 1) an die Mobilstation weiterleitet, welche aufgrund eines intern gespeicherten Schlüssels (Ki) hieraus eine Response 1 berechnet und an das Netz (N) absendet. Zur Authentisierung des Netzes (N) gegenüber der Mobilstation (M) ist vorgesehen, daß die an das Netz (N) zurückgesandte Response 1 gleichzeitig vom Netz (N) als Challenge 2 interpretiert wird, und daß das Netz (N) hierauf sofort eine Response 2 an die Mobilstation (M) sendet. Hierdurch wird der Datenverkehr zwischen der Mobilstation und dem Netz verbessert und beschleunigt, denn es wird auf die Übertragung der Challenge 2 zwischen Mobilstation und Netz verzichtet. Ebenso wird der Datenverkehr zwischen dem Netz und dem AUC verbessert, denn die Datenpaare Challenge 2 und Response 2 müssen nicht mehr im AUC gesondert berechnet und an das Netz weitergeleitet werden.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 98/01922

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 447 380 A (TELEFONAKTIEBOLAGET L M ERICSSON) 18 September 1991 see column 2, line 42 - column 4, line 17	1,3,4,14

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 December 1998	22/01/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Behringer, L.V.

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Ir ational Application No
PCT/DE 98/01922

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0447380 A	18-09-1991	SE 465800 B	28-10-1991
		AT 121254 T	15-04-1995
		AU 638820 B	08-07-1993
		AU 7495291 A	10-10-1991
		CA 2051385 A	10-09-1991
		CN 1054868 A,B	25-09-1991
		DE 69108762 D	18-05-1995
		DE 69108762 T	24-08-1995
		DK 447380 T	24-07-1995
		ES 2073726 T	16-08-1995
		FI 102134 B	15-10-1998
		HK 101895 A	30-06-1995
		IE 67887 B	01-05-1996
		JP 4505693 T	01-10-1992
		NO 300249 B	28-04-1997
		PT 96979 A,B	30-04-1993
		SE 9000856 A	10-09-1991
		WO 9114348 A	19-09-1991
		US 5390245 A	14-02-1995
		US 5282250 A	25-01-1994
		US 5559886 A	24-09-1996

INTERNATIONALER RECHERCHENBERICHT

In ationales Aktenzeichen
PCT/DE 98/01922

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/32 H04Q7/38

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 447 380 A (TELEFONAKTIEBOLAGET L M ERICSSON) 18. September 1991 siehe Spalte 2, Zeile 42 - Spalte 4, Zeile 17 -----	1,3,4,14

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
15. Dezember 1998	22/01/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Behringer, L.V.

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE 98/01922

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 0447380 A	18-09-1991	SE	465800 B	28-10-1991
		AT	121254 T	15-04-1995
		AU	638820 B	08-07-1993
		AU	7495291 A	10-10-1991
		CA	2051385 A	10-09-1991
		CN	1054868 A,B	25-09-1991
		DE	69108762 D	18-05-1995
		DE	69108762 T	24-08-1995
		DK	447380 T	24-07-1995
		ES	2073726 T	16-08-1995
		FI	102134 B	15-10-1998
		HK	101895 A	30-06-1995
		IE	67887 B	01-05-1996
		JP	4505693 T	01-10-1992
		NO	300249 B	28-04-1997
		PT	96979 A,B	30-04-1993
		SE	9000856 A	10-09-1991
		WO	9114348 A	19-09-1991
		US	5390245 A	14-02-1995
		US	5282250 A	25-01-1994
		US	5559886 A	24-09-1996